REMARKS

Claims 1-9,11-17,19-25, 27-30 and 42-50 were amended. No new claims have been presented. No new matter has been presented.

Rejections under 35 USC 112:

The Examiner rejected several claims under § 112, second paragraph, as indefinite. Applicants appreciate the Examiner's concern, but respectfully disagree. The claims and subject terms would be understood by those skilled in the art. Nonetheless, to alleviate the Examiner's concern and expedite allowance, please consider the following. Such amendments are presented solely for purpose of clarification and broaden the scope of the subject claims.

Claims 1, 7, 11, 15, 22, 30, 33 and 36 were amended. Support for the claims as amended can be found in paragraph [0084], lines 12-15 on page 34; see also paragraphs [0053, 0088-0095] of the specification.

Claim 7 was amended to comply with the examiner's comments. The term "much longer" is replaced with the term "longer" having a standard meaning. The support for this claim as amended can be found in paragraph [0065, 0074, 0084] of the specification.

Claims 11, 15, 22, 30 and 36 were amended by replacing the term "substantially greater" with the term "greater". The support for these claims as amended can be found in paragraph [0065, 0074, 0084] of the specification.

The term "about" was removed from claim 33. The support for this claim as amended can be found in paragraph [0053, 0094, 0099, 0108, 0143] of the specification.

Rejections under 35 USC 103:

Numerous claims were rejected under § 103 for reasons relating to obviousness. Again, Applicants' appreciate the Examiner's concern, but respectfully disagree. There is no motivation to combine the cited references. Without motivation, there is no *prima facie* obviousness. Even so, § 103 requires that obviousness be determined on the basis

of the claimed "subject matter as a whole." In this instance, the Examiner appeared not to have considered the entire subject matter of the claims at issue. Where, as here, the determination of obviousness is made on less than the entire claimed subject matter, there is no *prima facie* obviousness.

Nonetheless, as a matter of expediency, the following amendments are presented solely for purpose of clarification, without further limitation and to facilitate allowance of this application.

Claims 1-9, 11-17, 19-23, 27-29 and 48-50 were amended, as presented above.

Claims 1-9, 11-17, 19-23, 27-29 and 48-50 as amended are supported by the original disclosure, see, without limitation, paragraphs [0053] lines 11-17 on page 15, see also paragraphs [0009, 0013-0018, 0020-0021, 0094, 0099, 0108, 0143] of the original disclosure.

Claims 24-25 depend on Claim 22 and overcome the rejection once Claim 22 is amended.

Claims 30-35 were amended, as presented above. Claims 30-35 as amended are supported by the original disclosure, see paragraph, without limitation, [0053] lines 11-17 on page 15, see also [0020-0021, 0094, 0099, 0108, 0143] of the description.

Claims 36-47 were amended, as presented above. Claims 36-47 as amended are supported by the original disclosure; see, without limitation, paragraph [0053] lines 11-17 on page 15, see also paragraphs [0020-0021, 0094, 0099, 0108, 0143] of the description.

Without limitation, one aspect of the present invention can be considered encryption using multiple photons as opposite to the prior art encryption/key generation based on the use of single photon sources (or even less than one photon per channel use in the case of the Dultz *et al.* patent) in quantum channels. The prior art in this field, including the patents cited by the examiner, is based on embodiments of the BB84 protocol (see paragraph [7] in the specification) or its variants in various implementations. The BB84 protocol necessitates the use of single-photon states, which is very restrictive in most applications since optical amplifiers cannot be used with single-photon states. The present invention can use macroscopic quantum states of light

containing many photons – at least 10 on average – wherein the quantum noise of the large number can play a role in providing secrecy. Neither the prior art patent, nor the cited publication address or suggest the implementation of cryptographic schemes based on the use of quantum states of many photons, which is one distinguishing feature of the present invention.

Note that in the Dultz *et al.* patent cited by the examiner a single photon source is created by using a nonlinear crystal excited by a high-energy laser pulse (see column 2, lines 64-67). Thus, the high-energy laser pulse is simply a method of creating a single photon source and the quantum channel itself does not use multiple photons for key generation or encryption. Also note that in the Townsend patent a multi-photon source is used for publicly sending classical information between the two users (it is also used as a classical calibration signal), however the quantum channel for generating the key stream uses a single-photon source. That the Townsend patent uses a single-photon source for the quantum channel and a multi-photon source only for the public channel is stated in the abstract. Further note that the requirement of a public channel for discussion between the users, once the quantum transmissions with single photons have been completed, is a requirement of the BB84 protocol; no such requirement is present in the described method of direct encryption/key generation.

We again note that the use of macroscopic coherent states with many photons can allow the encrypted signals to pass through optical amplifiers. With the prior art, including the patents referenced by the examiner, one can not use optical amplifiers in key generation/encryption links. Townsend uses an electrical amplifier in his scheme (see for instance Figure 1) which is used in the electrical signal processing portion of the design and has nothing to do with optical amplification of a quantum-channel signal. The fact that AlphaEta signals of the present invention can be optically amplified makes such signals much more robust than those of the Dultz *et al.* and Townsend schemes. Consequently, data encryption/key generation over much longer distances becomes possible than those obtainable with the prior art techniques.

We further note that the Dultz *et al.* and Townsend patents both use only two basis states (four total possible states) chosen randomly by the users in order to generate a secret key. This is in fact a property of the 'BB-84'-like protocol of these types of prior art. The AlphaEta scheme differs from such methods in many ways. Firstly, without limitation, the AlphaEta system can be used for direct encryption. In contrast BB-84 generates a shared key which could in principle be used as a secret key in some other encryption system, but does not directly encrypt data. Secondly, AlphaEta can replace the randomly chosen set of just two basis states into a pseudo-randomly chosen set of many basis states. Although pseudo-randomly generating bit streams is a widely used tool (including a tool used in cryptography as shown in the Schneier reference cited by the examiner), it has not been used previously to select in which basis state to transmit a given quantum signal. Since we are choosing amongst a large group of possible basis states, we group the extended key output from the pseudo-random number generator into running keys of multiple bits. A different running key can then be used to choose a new basis state for every transmitted bit. Note that grouping an extended key generated from a traditional algorithm such as DES into multi-bit running keys for the purpose of encryption has no clear meaning in traditional encryption other than to modify the algorithm used into a slightly modified one, which still remains a fully algorithmic-based, deterministic encryption. In contrast AlphaEta fundamentally changes the encryption mechanism. Adding noise of many photons into the eavesdropper's observations makes such observations inherently noisy and thus inherently non-deterministic. This combination of traditional cryptographic tools with noisy macroscopic physical transmissions of many photons can greatly increase security, as described in the present invention. This concept and design will not be obvious to those knowledgeable in this field based on the prior art.

CONCLUSION

It is submitted that the present application is in form for allowance, and such action is respectfully requested.

Respectfully submitted:

Rodney D. DeKruif
Attorney for Applicants
Registration No. 35,853

Reinhart Boerner Van Deuren s.c.

1000 North Water Street, Suite 2100
Milwaukee, WI 53202
(414) 298-8360

Customer No. 22922